НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber war

February 2023

USAID
FROM THE AMERICAN PEOPLE

Prepared with the support of the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity.

This publication is made possible by the support of the American people through the United States Agency for International Development (USAID). The authors' views expressed in this publication do not necessarily reflect the views of USAID or the U.S. Government.

CONTENT

ACRONYMS 4

KEY TENDENCIES 5

1. FIRST WORLD CYBER WAR 9

Several Ukrainian state information resources targeted in a cyberattack 9

KillNet targets hospitals in countries supporting Ukraine during the war 9

Wired: Telegram vulnerable to control by russian intelligence services 9

Report on APT activities in the last four months of 2022 10

Belarusian hacker group leaks heaps of Roskomnadzor data 10

Google offers assessment of the first year into cyberwar 10

Websites of several German airports disrupted in a cyberattack 11

Hackers breach russian alert systems and spread false air strike warnings 11

Trustwave chalks up the first year into the cyberwar 11

CSIS: U.S. should use Ukraine's resilience experience to improve its own cybersecurity 12

russia's war against Ukraine undermines the ecosystem of cybercriminals 12

SecurityWeek publishes assessments of the first year into the cyberwar 12

CyberPeace Institute Research: DDoS attacks remain the most widely used tool in the first world cyberwar 13

Politico: russian cyber troops may resort to more damaging attacks in 2023 13

Dark Deal 2.0: cybercrime, russia, and the War in Ukraine 13

The West learns vital lessons from russia's cyberwar against Ukraine 13

Passion Botnet owners market its services to pro-russian hacker groups 14

russia-linked malware came close to shutting down American electrical and gas facilities last year 14

Danish hospitals targeted in an Anonymous Sudan cyberattack 14

2. CYBERSECURITY SITUATION IN UKRAINE 15

National Security and Defense Council (NSDC) Secretary Oleksiy Danilov presided over a meeting of the National Coordination Center for Cybersecurity 15

A representative of Ukraine will join the work of NATO's Cooperative Cyber Defence Centre of Excellence for the first time 16

NCSCC and NBU launched a project to counter cyber fraud in the financial sector 16

USAID will allocate $60 million to strengthen Ukraine's cybersecurity 16

russia commits over 10 cyberattacks on Ukraine a day. There were 1,500 of them since the beginning of the invasion – SBU 17

The XVII meeting of the national cybersecurity cluster discussed tendencies and new opportunities in this sphere of cybersecurity in 2023 ____ 17

In 2023, the NCSCC will conduct strategic-level sectoral command and staff training on cybersecurity and strategic communications ____ 18

Over 2,000 public servants from all over Ukraine learned to use OSINT instruments ___ 18

NCSCC experts held a working meeting with representatives of a French cybersecurity company ____ 18

“Ukraine is a shield against cyberattacks for the entire western world”– Illya Vityuk ___ 19

The State Service for Information Protection held UA30CTF student cybersecurity competition with EU support ____ 19

Law enforcement officers charged a russian blogger involved in propaganda ____ 20

Australian partners taught Ukrainian servicemen how to use OSINT methods ____ 20

The number of registered cyber incidents has grown almost three times in 2022, a report finds ____ 20

SSSCIP professionals continue to work with the world’s best cyber defense instruments ____ 21

Malicious cyber actors tried to steal data masquerading as Ukrainian MFA ____ 21

How do Western countries protect themselves from russian cyber aggression, Yuri Shchyhol writes for the Atlantic Council ____ 21

Targeted cyberattacks remain one of the main threats coming from FSB hackers, a report finds ____ 22

2,194 cyber incidents registered in Ukraine in 2022, the SSSCIP reports ____ 22

Cyber criminals attempted to spy on their target’s computers reportedly on behalf of Ukrtelecom ____ 22

A representative of the national SBU Academy took part in the U.S. DOE and CISA Cybersecurity in the Energy Sector training ____ 23

A training on using OSINT instruments for defense and security sector representatives was held with support from NCSCC ____ 23

Cyber police will cooperate with the Ukrainian national office on intellectual property and innovations ____ 23

ACRONYMS

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CERT-UA	Government Computer Emergency Response Team
CESER	Office of Cybersecurity, Energy Security, and Emergency Response (U.S.)
CISA	Cybersecurity & Infrastructure Security Agency
CRDF Global	Civil Research and Development Fund (U.S.)
CSIRT MON	Ministry of National Defence Computer Security Incident Response Team (Poland)
CSIS	Center for Strategic & International Studies (U.S.)
CTF	Capture the Flag
DARPA	Defense Advanced Research Projects Agency (U.S. Department of Defense)
DDoS	Distributed Denial-of-Service
DOE	U.S. Department of Energy
ENISA	European Union Agency for Cybersecurity
EU	European Union
FSB	Federal Security Service (Russian Federation)
GB	Gigabyte
HUMIT	Human Intelligence
ICS	Industrial Control System
IIoT	Industrial Internet of Things
INL	Idaho National Laboratory
IoT	Internet of Things
MaaS	Malware as a Service
MFA	Ministry of Foreign Affairs
NASK	National Science and Research Institute (Poland)
NATO	North Atlantic Treaty Organization
NCCC	National Coordination Cybersecurity Center
NIST	National Institute of Standards and Technology (U.S. Department of Commerce)
NSDC	National Security and Defense Council of Ukraine
OSINT	Open-source Intelligence
OT	Operational Technology
PSYOP	Psychological Operations
RaaS	Ransomware as a Service
SBU	Security Service of Ukraine
SSSCIP	State Service of Special Communications and Information Protection of Ukraine
TLP	Traffic Light Protocol
TTPs	Tactics, Techniques, and Procedures
TTX	Table Top Exercise
U.S.	United States
UA30CTF	Ukrainian Student Competition in Cybersecurity
UK	United Kingdom
USAID	United States Agency for International Development

KEY TENDENCIES

Countries of the world continue to modify their approaches to security based on the Russo-Ukrainian war experience. The European Union (EU) has intensified its efforts to launch its own satellite group to secure its government communications and is working more actively on the Cyber Resilience Act, specifically on the part related to the requirements for critical equipment at critical infrastructure facilities and is working to update cybersecurity standards. Taking into consideration Germany's new additional efforts to reduce its dependency on Chinese equipment as well as increased attention to protecting European cyberspace from foreign producers, there is a trend towards a policy of increased "sovereignisation" of European cyberspace.

Ukraine continues to identify targeted cyberattacks on its government sector. According to State Service for Special Communications and Information Protection (SSSCIP), 2.8 times more cyber incidents were recorded in 2022 than in 2021. And the number of information security events and the categories of "malicious code" and "malign information collection" grew by 18.3 and 2.2 times, respectively. To counter this increasing stream of attacks more efficiently, new practices to fight threats in cyberspace are being introduced (for example, a project to counter cyber fraud in the financial sector), and international assistance resources as well as resources of well-known international companies (Recorded Future) are involved.

Key Ukrainian agencies in charge of cybersecurity continue to develop interagency and international cooperation to prepare for a new wave of cyber confrontation with the russian federation. For this purpose, a table top exercise (TTX) on strategic communications and at least two secretarial cybersecurity TTX are planned in 2023. To increase the human resources potential in cybersecurity, the Ukrainian Student Competition in Cybersecurity (UA30CTF) exercise was held with 156 participants. In the international dimension, Ukraine is also intensifying its cooperation with NATO, with (a Ukrainian representative participating in the work of the Cooperative Cyber Defence Centre of Excellence (CCDCOE), as well as developing public-private partnerships, such as with cyber community representatives from the French private sector.

One more dimension on which cybersecurity agencies concentrate is teaching their professionals open-source intelligence (OSINT) techniques. A series of training for government sector representatives was held with the support of international partners: one involved over 2,000 participants from all regions of Ukraine and two were specifically for security and defense sector professionals.

International cooperation on common policies for digital development and cybersecurity has intensified. The lines of cooperation are increasingly tied to closer cooperation between Western countries and the Asia Pacific region, for example, an agreement between the EU and Singapore, activation of the Quad alliance, and intensified cooperation within the framework of #StopRansomware project.
Global cyber activity in February 2023 followed last year's trends. Ransomware remains the key problem for the majority of governments and private companies. Attackers expanded the use of their malicious code, creating new versions for Linux platform.

Attempts by government cybersecurity agencies to prevent threats and create instruments to unblock resources are only partially successful; attackers modify their code more quickly. The same big groups as in previous periods (e.g., LockBit, Lazarus, etc.) remain cyberattack leaders. Politically-motivated hacker activities continue to intensify, for example, hacking into the e-mail account of a British parliamentarian, an attack on an Israeli university, and a series of other incidents. The issue of supply chain attacks using open-source platforms attracts attention.

The possible use of artificial intelligence (AI) for malign purposes became an important topic of discussion in February. According to cyber professionals, systems like ChatGPT are already possibly used by states in their cyber activities. According to U.S. Department of Defense's Defense Advanced Research Projects Agency (DARPA), attacks on AI could become one of the key threats to human security in the near future, since dependence on this technology is only growing.

Another important cybersecurity trend is growing attention to Internet of Things (IoT) and Industrial Internet of Things (IIoT) security. These systems are increasingly used in production and everyday life and call for an increase in security. Against the background of threats to this sector identified as one of the key security trends in 2023, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) proposed "simplified cryptography" algorithms to protect small devices like this. This could be relevant to both industrial system and more traditional systems, such as automobile transportation, medical services, etc.

The production sector is increasingly concerned about possible mass escalation of ransomware attacks against Industrial Control System/Operational Technology (ICS/OT) systems. An 87% increase in the number of cyberattacks on industrial companies was recorded in 2022, and it is just a matter of time until it will reach their OT systems. OT equipment producers invest significant efforts into developing security patches for this equipment. The problem, however, is that many systems can no longer be modernized and better cybersecurity practices cannot be introduced. Another problem is the lack of cybersecurity culture for this kind of equipment at relevant enterprises.

In February 2023, cybersecurity companies identified several new advanced persistent threat (APT) groups or new campaigns run by known APT groups. These campaigns are similarly targeted at cyber spying operations in government institutions, research organizations, and a number of traditional sectors, namely energy, medicine, finance, and transportation (including shipping). Government agencies, such as the European Union Agency for Cybersecurity (ENISA), try to better understand which APT groups pose a threat to their countries and propose ways of better cooperation (for example, common approaches to responsible disclosure programs).

The world is summing up the first year of the cyberwar. Generally, the conclusions can be subdivided into three categories: assessment of Ukraine's actions and its readiness for the war, key characteristics of cyber rivalry during this year, and consequences and prospects for 2023.

Assessing Ukraine and its actions, experts indicate that Ukraine succeeded in avoiding the hardest consequences of cyberattacks and preventing large scale cyberattacks. Because Ukrainian cyber professionals turned out to be more effective than russian ones, Ukraine is succeeding to efficiently trace new threats. It is also important that the majority of important Ukrainian resources were transferred to the cloud. Experts also stress that the Ukrainian telecommunications sector has demonstrated resilience in the face of physical and cyber threats.

Characterizing the cyber rivalry itself, experts note that despite the significant effort russian hackers invested into gaining advantage in cyberspace, the results of their actions are inconclusive. Although russia actively combines cyber and information components and psychological operations (PSYOP), these efforts are also not efficient. The current concern that the cyber activity of both sides could spill over to other countries and their digital infrastructure only partially materialized. The number of attacks on Ukraine's partner countries have increased; however, they also fail to achieve destructive consequences. Experts also note that although cyberattacks did not play a noticeable role in the war, they helped both sides to collect a large amount of intelligence information that they were able to use in other spheres of confrontation.

As for the long-term consequences and prospects, significant changes in the Eastern European cybercrime ecosystem are already evident, and the activity of russian-speaking hacker communities has partially decreased. A "brain drain" of russian cyber professionals is being observed. A new wave of hacktivism (crowd hacktivism) has gained significant impetus. The most important conclusion in this sphere is that russia's capability to conduct destructive cyberattacks should not be underestimated. russian hacker groups have used this time to learn and possibly think of how to better conduct dangerous attacks. Therefore, the danger of more serious cyberattacks in 2023 persists and even increases.

A new grouping calling itself Anonymous Sudan has appeared on the hacker group map. It attacks European countries purportedly protesting against anti-Islamic actions. At the same time, researchers suspect that its participants are not Sudanese and the group itself was formed as a part of a russian information operation to complicate Sweden's NATO accession.

1. FIRST WORLD CYBER WAR

SEVERAL UKRAINIAN STATE INFORMATION RESOURCES TARGETED IN A CYBERATTACK

A number of web resources belonging to Ukrainian state and local authorities were attacked on February 23, resulting in modifications to the content of several pages. The Joint Response Team at the National Coordination Cybersecurity Center (NCSCC), consisting of experts from the SSSCIP, Security Service of Ukraine (SBU), and Cyber Police Department, collaborated to contain and probe the details of the cyber incident. Currently, it can be confirmed that the cyber incident did not cause any major disruption to system performance or government operations. The majority of affected information resources have been restored and are operating normally. Apparently, on the eve of the anniversary of the full-scale invasion, russia decided to yet again remind the world about its presence in cyberspace, where it has long behaved like a terrorist state, attacking civilian targets.

KILLNET TARGETS HOSPITALS IN COUNTRIES SUPPORTING UKRAINE DURING THE WAR

According to a report by Becker's Hospital Review published on February 2, the russian hacktivist network KillNet has been continuing to target hospitals in countries viewed as hostile to Russia. Their primary method of attack has been Distributed Denial-of-Service (DDoS), with medical facilities in the United Kingdom (UK), the Netherlands, the U.S., Germany, Poland, and Scandinavian countries targeted. The attacks have not caused significant damage thus far.

It has also been reported that the group has targeted at least 17 medical facilities in the United States. Patrick Sullivan, Chief Technology Officer for Security Strategy at cybersecurity company Akamai, commented to MedCityNews that while healthcare facilities typically have safeguards against ransomware and phishing, DDoS attacks are becoming an increasingly significant threat. He recommended that hospitals prepare response mechanisms by conducting drills.

WIRED: TELEGRAM VULNERABLE TO CONTROL BY RUSSIAN INTELLIGENCE SERVICES

On February 2nd, Wired published an article alleging that russian intelligence services had likely tampered with Telegram, a widely used messenger that is often regarded as secure due to its anonymity features. According to the article, police in russia have been targeting dissidents under circumstances that can only be explained by Telegram's apparent cooperation with russian authorities.

REPORT ON APT ACTIVITIES IN THE LAST FOUR MONTHS OF 2022

A report by ESET provides information about state-sponsored actors from China, Iran, North Korea, and russia. Specifically, the section on russia notes that APT groups linked to the country have been actively involved in cyber operations targeting Ukraine. These groups have deployed destructive ransomware and vipers, with the infamous Sandworm group using previously unknown ransomware to attack an energy company in Ukraine. APT groups are typically associated with state-sponsored actors, and the attack in question occurred in October, which coincided with russian military strikes against Ukraine's energy infrastructure. While there is no direct evidence of coordination between Sandworm and the russian military, the timing suggests that they may share similar goals.

The report details a new form of malware called NikoWiper, which was used in an attack against an energy company in Ukraine.

BELARUSIAN HACKER GROUP LEAKS HEAPS OF ROSKOMNADZOR DATA

On the night of February 15, a group identifying itself as the Belarusian Cyber Guerrillas released a 335 GB dump containing files and emails belonging to a department within Roskomnadzor's main radio frequency center.

The group claims that Roskomnadzor compiled data on protests in Ukraine and Kazakhstan, and evidence of this can be found on the group's Telegram channel. Prior to this, Reuters reported that Roskomnadzor had implemented an Oculus tool that enables

GOOGLE OFFERS ASSESSMENT OF THE FIRST YEAR INTO CYBERWAR

On February 16, Google's cybersecurity divisions (Threat Analysis Group, Mandiant, and Google Trust & Safety) published their findings on the primary trends observed throughout the year of conflict. They include:

- russian government-backed attackers have made significant efforts to gain an advantage in cyberspace, but the outcomes are frequently questionable;
- russia actively combines cyber and information components in its PSYOP;
- The war has resulted in significant changes in the Eastern European cybercrime landscape, including divisions based on political allegiances and geopolitics that are expected to have long-term consequences.

WEBSITES OF SEVERAL GERMAN AIRPORTS DISRUPTED IN A CYBERATTACK

On February 16, the websites of three German airports – Düsseldorf, Nuremberg, and Dortmund – were disrupted, following a major IT system failure at Lufthansa that caused extensive delays for thousands of passengers at Frankfurt Airport the day before. It is suspected that a DDoS attack was the cause of the disruption.

According to the russian media, on February 15, the pro-russian hacker group KillNet claimed responsibility for the Lufthansa disruption. The group's leader stated that the attack was carried out in retaliation for German Chancellor Olaf Scholz's decision to transfer Leopard tanks to Ukraine. Lufthansa, on the other hand, attributed the disruption to damaged broadband cables that were accidentally severed during construction work on a nearby railroad line. It should be noted that KillNet has a history of claiming responsibility for system failures and cyberattacks that may not have actually occurred or were ultimately unsuccessful.

Meanwhile, a group called Anonymous Sudan claimed responsibility for the cyberattacks against the German airports. The hackers posted a message on Telegram stating, "Bad weather for air traffic in Germany again," along with a list of their alleged victims.

HACKERS BREACH RUSSIAN ALERT SYSTEMS AND SPREAD FALSE AIR STRIKE WARNINGS

On February 23, a group of unidentified hackers breached the systems of several radio stations in russia, including Relax FM, Avatoradio, Yumor FM, and Comedy Radio. They also hacked the SMS messaging system and disseminated signals warning of an impending air strike. The message spread to numerous cities throughout russia, including Pyatigorsk, Tyumen, Voronezh, Kazan, Nizhny Novgorod, Magnitogorsk, Stary Oskol, Ufa, and Novouralsk.

TRUSTWAVE CHALKS UP THE FIRST YEAR INTO THE CYBERWAR

Trustwave, a cybersecurity company, published its first-year findings on the cyberwar on February 24. Its experts discovered that the cyber component did not play as large a role as initially anticipated. However, there was a noticeable concern that the cyber activity of both sides could potentially harm other countries and their digital infrastructures. To date, these fears have only partly materialized. The primary conclusion is that cyberattacks did not play a crucial role in the war but enabled each side to gather a significant amount of intelligence.

Trustwave's experts advise against underestimating russia's cyber capabilities. Although it has yet to launch any significant cyberattacks that have affected physical space, the country is learning from the ongoing war and could use new tactics, techniques, and procedures (TTPs) in future attacks. Trustwave is also revisiting the concept of establishing specific rules for cyber confrontations, such as those outlined in the Tallinn Manual.

CSIS: U.S. SHOULD USE UKRAINE'S RESILIENCE EXPERIENCE TO IMPROVE ITS OWN CYBERSECURITY

On February 24, Center for Strategic & International Studies (CSIS) experts published their recommendations for enhancing the cyber resilience of critical infrastructure and government agencies in the United States. They highlight the significance of Ukraine's experience in this field and the importance of implementing more effective risk management strategies. They emphasize that "cybersecurity involves managing risks rather than attempting to eliminate them."

They also identified several essential components of resilience, including information sharing, infrastructure investment, adopting a zero-trust architecture, public-private partnerships, cyber exercises (such as TTX), and increased focus on cybersecurity professionals.

RUSSIA'S WAR AGAINST UKRAINE UNDERMINES THE ECOSYSTEM OF CYBERCRIMINALS

A report by the Insikt Group, published on February 24, highlights the disintegration of groups like Conti in the Eastern European cybercrime community. While some members expressed support for the group, others criticized moscow's invasion of Ukraine. Additionally, russia experienced a "cyber brain drain" as some of its most active darknet users were mobilized into the military, leading to decreased activity in the russian-language darknet.

Recorded Future predicts that crowdsourcing activity is likely to play a significant role in the ongoing conflict between russia and Ukraine, with potential economic consequences. The researchers also argue that cybercrime, both in the post-Soviet space and globally, is entering a new era of instability due to russia's war against Ukraine.

SECURITYWEEK PUBLISHES ASSESSMENTS OF THE FIRST YEAR INTO THE CYBERWAR

In a February 24 article, journalists combined their own assessments and similar reports from a variety of sources to conclude that despite russia's systematic escalation of cyber activity, it has failed to achieve any significant results. Meanwhile, Ukraine is continuing to bolster its cyber defenses. Other findings include:

- russia's cyber activity against Ukraine has been substantial and is not abating;
- The activity of russian-speaking hacker communities has declined;
- There is an ongoing brain drain among russian cyber specialists (some of them were mobilized into the army while others left the country);
- Hacktivism (crowd hacktivism) gains momentum through the activities of groups like KillNet;
- The Ukrainian telecom sector has demonstrated resilience in the face of physical and cyber threats;
- Ukraine is effectively monitoring new threats;
- Critical systems have been moved into the cloud;
- Ukrainian cyber specialists have proven to be more effective than their russian peers.

CYBERPEACE INSTITUTE RESEARCH: DDOS ATTACKS REMAIN THE MOST WIDELY USED TOOL IN THE FIRST WORLD CYBERWAR

On February 24, the CyberPeace Institute published the results of its research into the cyber component of the russian-Ukrainian war. Its analysis of 1,100 cyberattacks revealed that nearly 80% were DDoS attacks. Furthermore, the organization's experts underscored the difficulty in ascertaining the actual impact of these cyber operations on individuals' lives and whether it is discernible.

POLITICO: RUSSIAN CYBER TROOPS MAY RESORT TO MORE DAMAGING ATTACKS IN 2023

In a February 25 article, Politico summarizes the available assessments of the first year of cyber warfare, based on research firms' published reports, and offers conclusions on potential trends for the upcoming year. Regarding the threat of more sever cyberattacks, Mark Montgomery, a Senior Fellow at the Foundation for Defense of Democracies' Cyber and Technology Innovation Department, believes that "russian malicious actors had just as little time to prepare their offensive operations as other actors in February 2022, and they were also uninformed about the true intentions of their leadership."

DARK DEAL 2.0: CYBERCRIME, RUSSIA, AND THE WAR IN UKRAINE

The INSIKT GROUP released a second report delving into the hidden connections between the russian federation, cybercriminals, and self-proclaimed hacktivists in russia and Eastern Europe during the ongoing conflict in Ukraine. The report, titled "Dark Deal: Ties between the russian State and Criminal Actors," is a continuation of their earlier publication from September 2021. Some of the report findings:

- There is a high likelihood that russian intelligence, military, and law enforcement agencies have established tacit agreements with cybercriminals who pose a threat. Additionally, in some instances, these agencies maintain structured and systematic relationships with cybercriminals through methods such as coercion, indirect collaboration, or recruitment.
- Cybercriminals are likely collaborating with Russia to coordinate or bolster russian offensive cyberinformation operations.
- russia's ongoing war in Ukraine has had a significant impact on various aspects of cybercrime, including alterations in the threat landscapes for malware-as-a-service (MaaS) and ransomware-as-a-service (RaaS), an increase in payment card fraud originating from russia, adjustments in cybercriminal targeting and infrastructure or hosting, and more.

THE WEST LEARNS VITAL LESSONS FROM RUSSIA'S CYBERWAR AGAINST UKRAINE

Yuriy Shchyhol, SSSCIP Chair, published an article in the Atlantic Council summarizing some of the lessons drawn by Ukraine from the russian cyberwar:

- The consequences of cyber attacks can be difficult to contain since decision makers may consider them as a zone weapon instead of a precision weapon, making them challenging to mitigate;
- Cyber attacks continue to remain in the "gray zone", where they can be used with fewer restrictions than kinetic strikes, are easier to deny, and harder to deter;
- Cyber operations are economical in terms of workforce;
- Supporting divisions can make a substantial contribution to offensive cyber operations;
- Cyber operations are hard to accomplish: both time and skills are needed to prepare and stage them.

PASSION BOTNET OWNERS MARKET ITS SERVICES TO PRO-RUSSIAN HACKER GROUPS

The Passion group, which is associated with KillNet and Anonymous russia, has reportedly started providing DDoS-as-a-service to pro-russian hackers. The Passion botnet was used in the January 27 attacks that targeted medical facilities across various countries, including the U.S., Portugal, Spain, Germany, Poland, Finland, Norway, the Netherlands, and the UK. The attacks were believed to be in response to these countries sending tanks to assist Ukraine.

The group asserts in its Telegram channel that it is neither directed nor funded by the russian government and solicits donations from followers to "achieve a shared mission." The new group is described in the Radware Cybersecurity Advisory.

RUSSIA-LINKED MALWARE CAME CLOSE TO SHUTTING DOWN AMERICAN ELECTRICAL AND GAS FACILITIES LAST YEAR

According to Robert M. Lee, founder and CEO of Dragos – a company that assists organizations in responding to cyberattacks – hackers from a group known as Chernovite attempted to use malware to target "roughly a dozen electricity and liquid natural gas facilities in the United States during the initial weeks of the war in Ukraine." Lee emphasized that the attack brought U.S. infrastructure closer to a shutdown than ever before, stating that the malware was a "state-level tool for wartime." However, he did not confirm whether the malware was successfully installed on the targeted networks during the attack or whether the hackers were only close to infiltrating the systems.

While Dragos adheres to a policy of not attributing hacker groups to specific states, other researchers have suggested that the malware described above is likely linked to Russia.

DANISH HOSPITALS TARGETED IN AN ANONYMOUS SUDAN CYBERATTACK

On the evening of February 27, a group identifying itself as Anonymous Sudan launched DDoS attacks against nine hospitals in Denmark, causing their websites to go down. Despite the disruption, Danish authorities confirmed that medical services were not affected. A few hours later, the hospitals announced that their websites had been restored.

The Anonymous Sudan group stated on Telegram that the attacks were carried out in response to the burning of the Quran. The group was referring to an incident in Stockholm where Rasmus Paludan, a Danish and Swedish citizen described as a "far-right politician and anti-Islamic provocateur" by The Guardian, set fire to the holy book in front of the Turkish embassy.

2. CYBERSECURITY SITUATION IN UKRAINE

NATIONAL SECURITY AND DEFENSE COUNCIL (NSDC) SECRETARY OLEKSIY DANILOV PRESIDED OVER A MEETING OF THE NATIONAL COORDINATION CENTER FOR CYBERSECURITY

At the meeting, participants discussed the possible escalation of russian cyber aggression against Ukraine and the primary measures to counter it under the conditions of martial law, results of the command and staff exercises National Cyber Readiness-2022, and amendments to the General Rules for the Exchange of Information on Cyber Incidents, i.e. Traffic Light Protocol (TLP).

According to the NSDC secretary, just like a year ago, the offensive in cyberspace could come before and continue during the new wave of russia's large-scale aggression and Ukraine needs to be ready to repel it.

Oleksiy Danilov said that Ukraine has strengthened and developed the national cybersecurity system and has significantly improved the technical equipment of the Ukrainian military and cyber warriors. In this context, he thanked all institutions in charge of cybersecurity, NCSCC in particular, for coordinated efforts, protecting cyberspace, preventing cyber incidents, and minimizing their consequences.

Danilov also stressed that Ukraine has built up its position as a full-fledged partner in international cooperation in the cybersecurity sphere. He mentioned the agreement between Ukraine and NATO's Cooperative Cyber Defence Centre of Excellence. Ukraine's membership in this center, he said, will intensify the exchange of cyber experience between Ukraine and other NATO CCDCOE member countries. Furthermore, this is an important step on Ukraine's path to NATO membership.

The NSDC secretary also drew attention to the importance of training cybersecurity professionals. They also discussed the importance of strengthening the legal basis for increasing the capabilities of the national cybersecurity system to counter cyber threats.

The meeting participants adopted a new edition of the General Rules for the Exchange of Information on Cyber Incidents (TLP).

A REPRESENTATIVE OF UKRAINE WILL JOIN THE WORK OF NATO'S COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE FOR THE FIRST TIME

At a meeting on February 17, 2023, the Cabinet of Ministers supported the SSSCIP's proposal and adopted the resolution "On a representative of the State Service for Special Communications and Information Protection to NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE)."

In the future, representatives of other institutions that are a part of to the national cybersecurity system, namely the Ministry of Defense and the SBU, are also expected to participate in the CCDCOE on a rotational basis.

Ukraine's representative in CCDCOE will facilitate information exchange and increase the efficiency of countering aggression in cyberspace. Ukrainian professionals will have access to an extensive knowledge base and will be able to participate in joint cyber exercises and conduct research with partners on cybersecurity, in particular, on critical infrastructure protection.

NCSCC AND NBU LAUNCHED A PROJECT TO COUNTER CYBER FRAUD IN THE FINANCIAL SECTOR

The project's main goal is to improve the protection of citizens from cyber criminals, whose activity has significantly intensified during martial law in Ukraine. The attackers conduct phishing campaigns to coax bank credentials in order to steal money. The promises the attackers give to their victims vary depending on the current news, specifically those relating to government and international financial aid to citizens.

The project's task is simple: decrease the number of users who go to fraudulent sites by sending them to a page with a warning that the site was created by attackers. In the first month alone, about 120,000 unique users landed on the web page. In other words, tens of thousands of Ukrainian citizens per month will be protected from being hooked by cyber fraudsters and potentially being defrauded.

In the autumn 2022, the NCSCC set up a working group consisting of representatives of government agencies and providers with the biggest infrastructure. A successful test was conducted of the system to protect from financial phishing. Kyivstar was the first of the biggest providers to join the project. Now, all operators that care about the clients' cybersecurity have joined the protective system.

USAID WILL ALLOCATE $60 MILLION TO STRENGTHEN UKRAINE'S CYBERSECURITY

Vice Prime Minister-Minister of Digital Transformation Mykhailo Fedorov met with USAID Deputy Administrator Isobel Coleman. They discussed further cooperation between Ukraine and the U.S. Agency for International Development (USAID), in particular, strengthening cyber defense and support for digital transformation.

USAID said that it will allocate $60 million to strengthen Ukraine's cybersecurity. This will help the government protect critical infrastructure facilities from russian cyberattacks, in particular, energy, telecommunications, and data storage systems.

"USAID is a reliable partner of Ukraine. Thanks to the agency's support we have launched the application and the Diia portal, as well as the ten most popular services that Ukrainians can get in just several clicks. The Digital Transformation Ministry's team actively works with USAID in the sphere of digital transformation and cybersecurity. With the Agency's support, we create the most convenient services for Ukrainians in Diia, and we share our experience with the world. We are grateful to USAID for regular help, support for our digital initiatives and strengthening the state's cybersecurity," Mykhailo Fedorov said.

RUSSIA COMMITS OVER 10 CYBERATTACKS ON UKRAINE A DAY. THERE WERE 1,500 OF THEM SINCE THE BEGINNING OF THE INVASION – SBU

Ukraine is fighting with the increased number of cyberattacks while Russia commits at least 10 attacks a day, the head of Ukraine's Security Service Vasyl Maluk told The Independent. According to him, 4,500 cyberattacks have been recorded since the start of the invasion.

"Currently, Russia commits over 10 cyberattacks a day on average. Their targets differ and include government resources, critical infrastructure facilities, and so on. However, we successfully counter the adversary in cyberspace", he said.

According to Maluk, the agency recorded 800 cyberattacks in 2020, and in 2021 the number was about 2,000; after the invasion, it grew to over 4,500. He added that there are different types of attacks, sometimes there are mass attacks.

THE XVII MEETING OF THE NATIONAL CYBERSECURITY CLUSTER DISCUSSED TENDENCIES AND NEW OPPORTUNITIES IN THIS SPHERE OF CYBERSECURITY IN 2023

The XVII meeting of the national cybersecurity cluster "Cybersecurity 2023: Tendencies, New Opportunities, and Prospects" took place on February 21, 2023. The event was organized by the NCSCC and the U.S. Civilian Research and Development Foundation with the support of the U.S. Department of State.

In his opening remarks, Serhiy Prokopenko, head of the directorate for ensuring the functioning of the NCSCC, said that the national cybersecurity cluster as a coordination activity has shown its effectiveness. Thanks to its efforts, government agencies and critical infrastructure facilities received the needed support, in particular, through grant programs. And in 2023, the cluster team will continue this work.

"In 2022, thanks to the coordinated joint efforts of the state, private sector, and international support, Ukraine proved its resilience in cyberspace. We currently observe a decrease in the number of cyberattacks compared to last year, however, the threat level has not decreased. Enemy attacks have become more intricate and sophisticated and pose bigger risks. This is why the issue of cybersecurity remains among the most important on the agenda and is at the center at all levels, starting from technical professionals and up to manager level at all agencies involved in cybersecurity", Prokopenko said. He also presented NCSCC priorities, technological projects, and activity plans for 2023.

Over 300 representatives of the government, international and donor community, embassies, and private institutions joined the discussion of tendencies and new opportunities in cybersecurity in 2023. Representatives of the Ministry for Digital Transformation, NATO office in Ukraine, the U.S. Army's Center for Engineering Research and Development, Australian company Internet 2.0, and others were among the key speakers of the event.

IN 2023, THE NCSCC WILL CONDUCT STRATEGIC-LEVEL SECTORAL COMMAND AND STAFF TRAINING ON CYBERSECURITY AND STRATEGIC COMMUNICATIONS

NSDC Deputy Secretary Serhiy Demedyuk summed up the results of the command and staff exercises on cybersecurity at the strategic level "National Cyber Readiness 2022" (December 2022) at the NCSCC meeting on February 9, 2023. Representatives of all government institutions whose heads are members of the NCSCC and other government agencies and critical infrastructure facilities participated in the meeting.

Regularly conducting this kind of exercise is mandated by the implementation plan for Ukraine's cybersecurity strategy. "The command and staff exercises allowed coordinating the actions of all agencies involved in providing cybersecurity and work out joint actions at a sufficient level. At the same time, it is necessary to make urgent decisions to improve the organization and conduct of the command and staff exercises at the strategic level, and introduce the practice of command and staff exercises on cybersecurity in specific spheres," Demedyuk said.

During the current year, the NCSCC has to ensure annual strategic level command and staff exercises on cybersecurity and on strategic communications are conducted and at least two command and staff exercises in specific spheres.

OVER 2,000 PUBLIC SERVANTS FROM ALL OVER UKRAINE LEARNED TO USE OSINT INSTRUMENTS

The NCSCC, with the support of the U.S. Civil Research and Development Fund (CRDF Global) and the U.S. Department of State, held the 3-day online training "OSINT – intelligence using open sources." Over 2,000 government sector representatives from all regions of Ukraine participated.

Due to the large number of interested participants, the training was held online in two stages, on February 8-10 and February 22-24. Together with leading practical researchers of the Ukrainian company Molfar, the participants discussed the latest research and did practical assignments on the following topics: open-source searches, contact search, using Telegram bots, PSYOP and their use as a method of information warfare, image analysis, and human intelligence (HUMINT) or social engineering.

A representative of the French Predicta Lab gave the lecture "GEOINT – the art of geolocation."

NCSCC EXPERTS HELD A WORKING MEETING WITH REPRESENTATIVES OF A FRENCH CYBERSECURITY COMPANY

The head of the NSDC Information Security and Cybersecurity Service, NCSCC Secretary Natalia Tkatchuk, and the head of the directorate for ensuring the functioning of NCSCC Serhiy Prokopenko met with private sector representatives of the French cybersecurity community, including Cyber Task Force, Gatewatcher, and Predicta Lab. Representatives of the French Embassy to Ukraine and Ukrainian business also took part in the event.

"One of NCSCC's priorities is to develop public-private partnership in Ukraine and in the international arena. Last year, we significantly strengthened Ukraine's positioning as a full-fledged partner of international cooperation in the cybersecurity sphere. We feel the support of democratic countries and are interested in cooperating with the French side to develop Ukraine's national cybersecurity sphere," Natalia Tkachuk said.

In the meeting, special attention was paid to cooperation in cybersecurity, opportunities for exchanging experience, and launching joint educational projects.

“UKRAINE IS A SHIELD AGAINST CYBERATTACKS FOR THE ENTIRE WESTERN WORLD”– ILLYA VITYUK

Ukraine is the country with the absolute majority of russian cyberattacks currently focused on it. So far in 2023, SBU cyber professionals have neutralized over 550 threats. Head of the SBU Cybersecurity Department Ilya Vityuk reported this on air during the national telethon.

He noted that our western partners understand that if Ukrainian cyber defense had fallen, the entire enemy cyber capability would have been targeted at them. “If we neutralized over 4,500 cyberattacks and critical cyber incidents last year, in a month and half this year, we already had 550 attacks of this kind. This means russia maintains the speed and the scale. However, we stopped most of the cyberattacks at their initial stages,” Vityuk stressed.

According to him, the main targets of enemy cyberattacks are logistical objects and transportation, Ukraine’s energy sphere, military objects, information resources, and government registers.

As the head of the SBU Cybersecurity Department stressed, the russian federation has constantly attacked Ukraine since 2014. “However, our Security Service has evolved a lot more than the russians did. The very fact that the majority of Ukrainian systems work normally is clear evidence that we successfully deal with the challenges, even in the most difficult psychological conditions and with the shortage of electricity. International partner support also helps Ukraine to counter the enemy efficiently.”

“In this war, not only do we repel the russian occupiers’ attacks, but also efficiently counterattack ourselves. An important goal is to get intelligence information for Ukraine’s military forces. However, sometimes we simply let them have it, respond to their aggression symmetrically, and even a lot more powerfully,” Illya Vityuk summed up.

THE STATE SERVICE FOR INFORMATION PROTECTION HELD UA30CTF STUDENT CYBERSECURITY COMPETITION WITH EU SUPPORT

The State Service for Information Protection, supported by the EU-financed project EU4DigitalUA, held the UA30CTF cybersecurity competition. 156 third- and fourth-year students from 22 Ukrainian higher educational institutions participated in the competition.

4n0M4lY team, from the National Technical University of Ukraine Ihor Sikorsky Kyiv Polytechnic Institute, won first place. Second and third places went to the Ghost of Sheva (Kyiv National Taras Shevchenko University) and Silent Sparrow (Vadym Hetman Kyiv National Economic University, Ukraine University, and the National Technical University of Ukraine Ihor Sikorsky Kyiv Polytechnical Institute) respectively.

The competition was styled after #Jeopardy Capture the Flag (CTF) game. For six hours, the teams worked on 25 problems meant to both test logic and find and exploit vulnerabilities while solving interesting logical problems.

“One of the priorities of the State Service for Special Communications and Information Protection in reforming the cybersecurity sphere is to develop human resource potential. In particular, raising the preparation level of future employees. For this purpose, the State Information Security Service not only started reforming formal education but also holds practical events similar to this where students can apply their knowledge in a competition format. I hope in the future there will be more events like this in Ukraine,” said SSSCIP Deputy Head Victor Zhora.

LAW ENFORCEMENT OFFICERS CHARGED A RUSSIAN BLOGGER INVOLVED IN PROPAGANDA

In his media reporting, the suspect justifies russia's armed aggression against Ukraine and spreads fake news, disinformation, and russian propaganda. According to Ukrainian legislation, the perpetrator faces up to five years in prison.

His illegal activities were documented by Cyber Police Department officers, the Main Investigative Directorate of the National Police, and officers of the Prosecutor General's Office of Ukraine.

The russian video blogger created propaganda materials for the WarGonzo project on YouTube and a pro-russian Telegram channel. In particular, he justified russia's armed aggression against Ukraine and the occupation of the country and spread fakes and disinformation. The overall size of the propaganda project's audience on different Internet resources is about 3 million users and the number of views exceeds 500 million.

AUSTRALIAN PARTNERS TAUGHT UKRAINIAN SERVICEMEN HOW TO USE OSINT METHODS

Australian company Fivecast held a training for Ukraine's defense sector professionals in Kyiv. Deputy Defense Minister for Digital Development, Digital Transformation, and Digitalization Oleh Haiduk was present at the event. He thanked the international partners for support and stressed the importance of the joint mission to protect the entire world from russia's aggression. The event took place with support from the governments of Australia and the United Kingdom.

During the practical training, participants were shown the capabilities of modern search methods in looking for different types of information online. Service members of different Defense Forces components learned to apply the suggested software to practice making information requests on different issues.

THE NUMBER OF REGISTERED CYBER INCIDENTS HAS GROWN ALMOST THREE TIMES IN 2022, A REPORT FINDS

The State Cyber Defense Center registered 2.8 times more cyber incidents in 2022 than in 2021. The number of information security events in the categories of "malicious code" and "malicious information collection" grew 18.3 and 2.2 times respectively.

This information was made public in the annual report of the system to identify vulnerabilities and react to cyber incidents and cyberattacks. Over the last year, the system:

- Processed about 58 billion events received with the help of monitoring analysis and transfer of telemetric information about cyber incidents and cyberattacks;
- Detected 181 million suspicious information security events (with preliminary analysis);
- Processed 179 critical information security events (potential cyber incidents, detected by filtering suspicious information security events and secondary analysis);
- Security analysts directly recorded and processed 415 cyber incidents (critical information security events).

SSSCIP PROFESSIONALS CONTINUE TO WORK WITH THE WORLD'S BEST CYBER DEFENSE INSTRUMENTS

Thanks to international assistance, SSSCIP professionals had the opportunity to use advanced global cybersecurity instruments to protect Ukraine. In 2022, the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity helped to pay for the 2023 license for several Recorded Future's Intelligence Cloud Platform modules.

Recorded Future Intelligence Cloud is a product that helps collect data, analyze behavior, and detect malicious actions and infrastructure and their goals in cyberspace. The platform is also used for the system to detect vulnerabilities and react to cyber incidents and cyberattacks.

MALICIOUS CYBER ACTORS TRIED TO STEAL DATA MASQUERADING AS UKRAINIAN MFA

The Ukrainian government Computer Emergency Response Team (CERT-UA) detected a web page that imitates the official web portal of the Ministry of Foreign Affairs (MFA). The page offers its visitors to download an app to detect infected computers. In reality, the link hides malicious code.

If someone follows the link, the computer downloads a BAT-file "Protector.bat", which will lead to downloading and launching on the computer PowerShell scripts that search for files with the following extensions: .edb, .ems, .eme, .emz, .key, .pem, .ovpn, .bat, .cer, .p12, .cfg, .log, .txt, .pdf, .doc, .docx, .xls, .xlsx, .rdg. It will then make screen shots and transfer them to the malicious server.

In cooperation with CERT Polska and Poland's Ministry of National Defence Computer Security Incident Response Team (CSIRT MON), similar fishing resources that imitate the official web pages of Ukraine's MFA and SBU and Polish police were detected. In June 2022, a similar phishing webpage imitated the web interface of Ukraine's Ministry of Defense mail server. The activity is being tracked with UAC-0114 identifier (also known as Winter Vivern).

HOW DO WESTERN COUNTRIES PROTECT THEMSELVES FROM RUSSIAN CYBER AGGRESSION, YURI SHCHYHOL WRITES FOR THE ATLANTIC COUNCIL

russian cyberattacks may lead to undermining and blocking the work of government agencies and critical infrastructure, manipulating public opinion, and spreading malicious code through hacked e-mail accounts, SSSCIP Head Yuri Shchyhol wrote in his Atlantic Council piece.

"While more traditional acts of aggression can provoke a strong response, cyberattacks operate in a 'gray zone' that makes them convenient for the kremlin, which is trying to cause as much chaos as possible in Europe and North America without running into a direct military response," the SSSCIP head notes.

He believes that Western countries should take Ukrainian experience into account while countering russian cyber aggression. In particular, to counter attacks on time, it is extremely important to coordinate efforts with civil society and exchange information with a wide range of stakeholders. However, this is not enough to stop cyber aggression in the entire world. More decisive change is needed. Cyberattacks should be treated as regular military aggression and should elicit the same noncompromising reaction. If this does not happen, even if putin is defeated in Ukraine, other authoritarian countries may follow russia's way.

TARGETED CYBERATTACKS REMAIN ONE OF THE MAIN THREATS COMING FROM FSB HACKERS, A REPORT FINDS

Professionals of the SSSCIP State Cyberdefence Center analyzed malicious code GammaLoad and GammaSteel used by the UAC-0010 (Gamaredon, Armageddon, Primitive Bear) group in its attacks. Attackers use GammaLoad and GammaSteel for targeted attacks on Ukrainian government agencies and critical information infrastructure facilities.

The malign activity tracked by the UAC-0010 identifier is carried out jointly with former SBU officers in the Autonomous Republic of Crimea who currently work for a russian federation Federal Security Service (FSB) unit in Crimea. To remain undetected by cyber protection means built on signature analysis, the attackers constantly perfect their tactics and modify the malicious code. Consequently, targeted cyberattacks remain one of the key cyber threats in Ukraine.

The information made public in the report once again stresses the need to proactively detect threats based on behavioral analysis.

2,194 CYBER INCIDENTS REGISTERED IN UKRAINE IN 2022, THE SSSCIP REPORTS

In 2022, SSSCIP professionals registered over 2,000 cyber incidents and an even greater number of cyberattacks in Ukraine, SSSCIP Deputy Head for Digital Development, Digital Transformation, and Digitalization Viktor Zhora told Suspilne public television in an interview.

“Cyberattacks happen because we have a full-fledged cyber war. The first cyber war in the world. It started nine years ago, practically immediately after the annexation of Crimea and the occupation of the eastern part of the Donbas. Its active phase is underway currently. Practically starting from January 14, 2022, we have been under a constant stream of attacks and we counter them quite effectively,” the official said.

He believes that it is possible to prevent cyberattacks by employing a set of measures that “includes special cyber defense complexes, cooperation between key entities responsible for ensuring cybersecurity, timely reaction to cyber incidents, and following cyber hygiene rules and the recommendations of cybersecurity experts,” the official explained.

CYBER CRIMINALS ATTEMPTED TO SPY ON THEIR TARGET’S COMPUTERS REPORTEDLY ON BEHALF OF UKRTELECOM

CERT-UA recorded a mass mailing of electronic messages reportedly from Ukrtelecom. Aimed primarily at the government sector, the mailing most likely was meant for spying purposes.

The detected activity has been traced by the UAC-0050 identifier at least starting from 2020. Previously, the group carried out its attacks with the remote administration tool RemoteUtilities. Based on the program’s functions and the fact that the cyberattack usually (but not exclusively) targets Ukrainian government agencies, CERT-UA professionals believe that the activity is being carried out for spying purposes.

A REPRESENTATIVE OF THE NATIONAL SBU ACADEMY TOOK PART IN THE U.S. DOE AND CISA CYBERSECURITY IN THE ENERGY SECTOR TRAINING

The international training for cybersecurity of automated technological process control systems in the energy sector “Introduction to Control Systems Cybersecurity Training” was organized by the Polish National Science and Research Institute (NASK); U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER); and Cybersecurity and Infrastructure Security Agency (CISA).

The educational materials provided to the training participants were developed by DOE Idaho National Laboratory (INL). The work on practical cases was done with the help of modified virtual environment and the training itself was conducted by top international cyber defense professionals.

A TRAINING ON USING OSINT INSTRUMENTS FOR DEFENSE AND SECURITY SECTOR REPRESENTATIVES WAS HELD WITH SUPPORT FROM NCSCC

On February 10, 2023, a training was held for representatives of the defense and security sector on using OSINT instruments in the interests of law enforcement, national security, and defense.

Officers of the National Police of Ukraine, SBU, and cadets of the SBU National Academy took part in the event supported by the NCSCC and the National Academy of the Security Service of Ukraine.

“Cooperation with the private sector and Ukraine’s leading educational institutions is one of and NCSCC’s priorities in this sphere of building up the potential of the national cybersecurity system. We regularly hold educational sessions to enhance the competences of the government sector employees and are grateful to everybody who helps us with this”, the head of the Information Security and Cybersecurity Service of the and NSDC apparatus, NCSCC Secretary Natalia Tkachuk noted.

CYBER POLICE WILL COOPERATE WITH THE UKRAINIAN NATIONAL OFFICE ON INTELLECTUAL PROPERTY AND INNOVATIONS

Training, seminars and exercises to counter crimes in intellectual property are planned within the partnership.

Yuriy Vykhodets, head of the Cyber Police Department, held a working meeting with representatives of the state government organization “Ukrainian national office for intellectual property and innovations.” The parties discussed outstanding issues related to Internet piracy, illegal rebroadcasting of television channels, and the spread of illegal content online.

Yuriy Vykhodets noted that the Cyber Police cooperate with the largest media corporation in the country and builds public-private partnerships because protecting intellectual rights is a complicated issue that calls for an all-around approach.